PC Professional

A SURVIVAL GUIDE

SMALL BUSINESS CYBERSECURITY

A LOOK AT MODERN DAY CYBERCRIME AND THE ESSENTIAL PRECAUTIONS EVERY BUSINESS MUST TAKE

Contents

Introduction

In today’s digital age, small businesses are more connected than ever. From online banking and customer databases to cloud platforms and email communication, technology plays a vital role in daily operations. However, this increased reliance on digital systems has introduced a rising risk: cybercrime.

Contrary to common belief, cybercriminals do not focus solely on large corporations. Small and mid-sized businesses (SMBs) are frequent targets precisely because they often lack enterprise-grade protections. In fact, nearly half of all cyberattacks are directed at small businesses, resulting in financial loss, reputational damage, and operational downtime.

Cyber threats come in many forms: phishing emails, ransomware, weak passwords, and more. Fortunately, you don’t need to be a cybersecurity expert to protect your business. With the right guidance and proactive measures, you can significantly reduce risk.

This guide outlines key cybersecurity threats, essential protections, and actionable strategies tailored for small businesses. Whether you're a sole proprietor or managing a growing team, the insights here will help strengthen your digital defenses and safeguard your operations.

History of Cybercrime

“Over the history of mankind, whenever something new has been deployed for good, there have been people that have twisted that new functionality and redeployed it for evil.”

1969 - ARPANET is Invented

The first computer network, consisting of 6 computers.

1971 - Creeper/Reaper

The first computer virus, “Creeper,” is developed as an experiment. In response, “Reaper,” the first antivirus, is created.

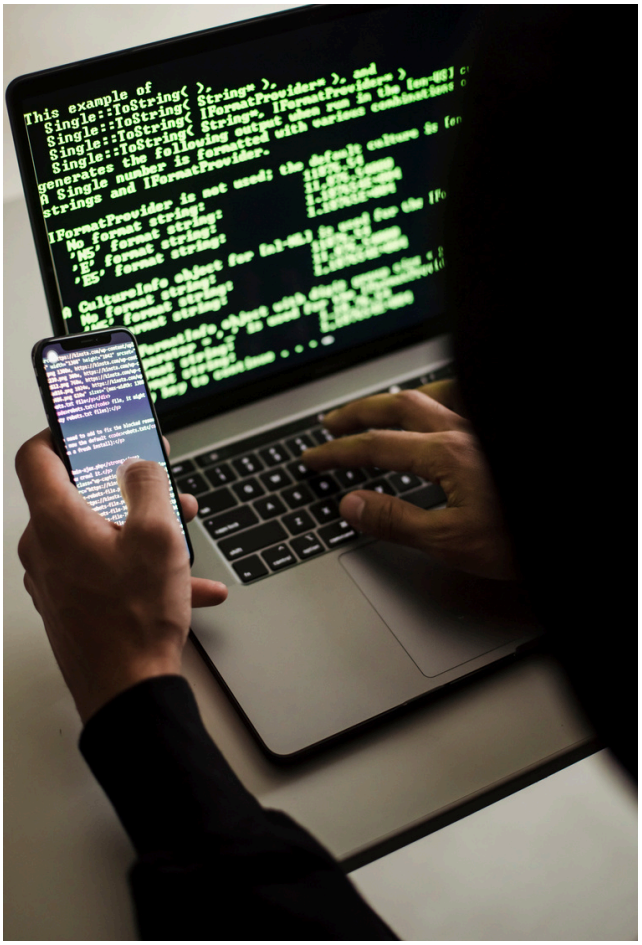
1988 - The ‘Morris Worm’

The Morris Worm marks the first major prosecution of cybercrime. This event shifted perceptions, making it clear that cybercrime posed a real-world threat.

While email revolutionized communication, it also became an effective delivery mechanism for malicious software. Over time, cybercrime grew from isolated incidents to a coordinated global threat.

Cybercrime & Organized Crime

“Cybercriminals today operate with the structure and coordination of professional organizations. Sophistication increases year over year, while many small businesses lack the resources to keep pace.”



Several societal factors contribute to this vulnerability:

- The average person owns four internet-connected devices.
- The volume of data accessible online continues to grow exponentially.
- Cybersecurity budgets often lag behind threat sophistication.
- Cybercrime is now more profitable than the illegal drug trade and is projected to cost the global economy $10 trillion annually by 2025.

Attacks are no longer random. Criminal groups conduct extensive research, identify weak entry points, and deploy well-crafted phishing campaigns tailored to specific targets. Once inside, other members execute malware attacks, encrypt data, and manage ransom payments. These operations are methodical—and profitable.

Cybercrime has become sophisticated and organized

- 1st group: Stakes out the business, does diligent research, finds the most vulnerable entry-point. They target a specific person/position within the organization.

- 2nd group: Writes email targeting that vulnerable person, creating copy designed specifically to entice that person into clicking or opening link/attachment.
  - These are intelligent, manipulative emails, appealing to their emotions so that their emotion supersedes their logic.
  - They act without thinking because they are stressed, fearful, excited, etc.

- 3rd group: Works on malware to infect network, encrypts data, and sends ransom message.

- 4th group: The accounts payable group. They will receive the ransom payment.

These attacks are orchestrated with business-like precision, involving multiple groups with distinct roles.

Case Study:

Riviera Beach, Florida

In 2019, the city of Riviera Beach, Florida, paid a $600,000 ransom following a ransomware attack. The breach was attributed to:

- Outdated computer systems
- Temporary leadership in key IT and governmental roles
- A delay in deploying a new $800,000 IT infrastructure

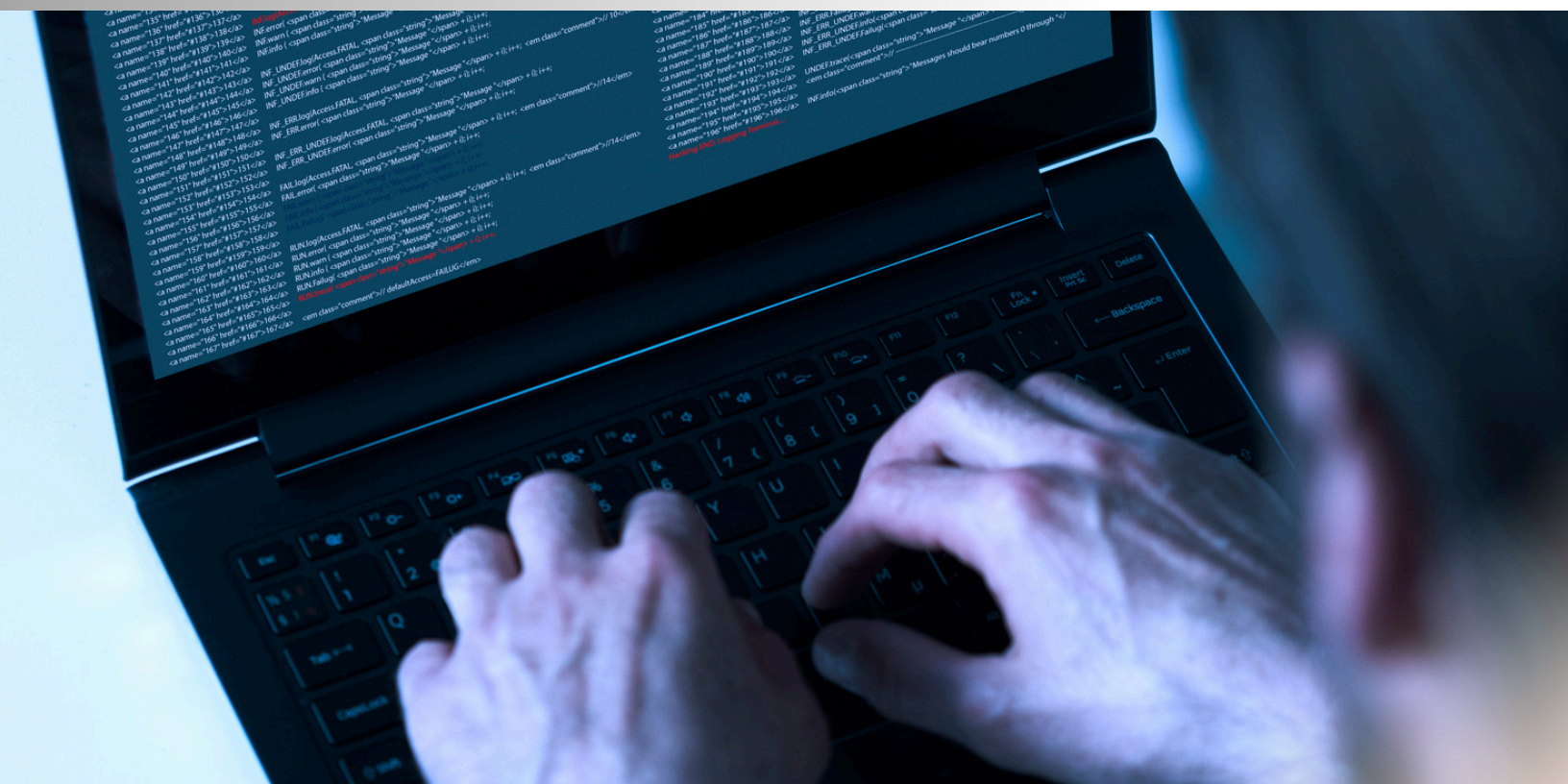
The incident underscores a critical truth: timely implementation of cybersecurity measures is essential. Even substantial investments offer little protection if they aren't in place before an attack.

New Breed of Cybercrime

While data remains the main target for hackers, a ransom is not always the main goal.

Cybercriminals increasingly look to destroy data, or even change it in an attempt to create confusion and breed mistrust.

The most sophisticated hackers enter the network and remain undetected, simply watching and learning everything they can about the organization.



Why Small Businesses are The #1 Target

Small businesses account for 90% of the U.S. economy.

Many falsely believe they are too small to be hacked, or do not have anything of value for hackers. Consequently, they believe they don't need rigorous cybersecurity.

They either don't know about their risk, or they believe they know enough to protect themselves.

In today's digital landscape, cybersecurity must be looked at as a strategy. It's not IF, but WHEN.

You are not too small to be hacked; you are just too small to make the news.

Common factors that leave small businesses exposed:

- **Lack of resources:** IT is often the first area cut during budget reductions.
- **Lack of awareness:** Business leaders may underestimate their risk or overestimate their in-house IT expertise.
- **Overreliance on informal IT support:** A single "IT person" often isn't equipped to handle sophisticated threats.

Most Common Cybercrimes

Ransomware

- Encrypts company data and demands payment for restoration—commonly triggered by phishing emails.

Data Breaches

- Unauthorized access to sensitive data via phishing, third-party software, or weak credentials.

Brute Force Attack

- Automated programs attempt to guess passwords until access is gained.

80% of SMBs express concern about cybersecurity, yet only one-third take proactive steps. Of those, many implement insufficient protections.

Cybersecurity is achievable. It starts with awareness and the understanding that layered defense is more effective than any single solution.

9 key things businesses should know to protect themselves:

- A Single-layer approach to cybersecurity is not a strategy: Utilize a multiple-layer solution.
- Perform risk assessments quarterly. What is measured is known. Don't rely on what was effective against yesterday's enemy.
- Out of those assessments, you need to identify critical systems and vulnerabilities that directly impact the business.
- Address all loopholes that were found during the assessments.
- Perform end-user training and phishing simulations weekly. A fire door isn't effective if the employee doesn't know how to close it.
- The right toolset for the job includes next-generation protection and managed detection.
- Business Continuity and Disaster Recovery Plan: Get your business back up and running within a matter of hours not days.
- Penetration Testing: perform annually. A third-party forces an attack from the outside and within.
- Cyber Liability Insurance.

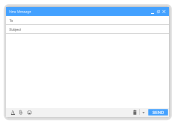
Phishing & Social Engineering

The #1 way cybercriminals hack into your network: PHISHING

How to identify phishing attacks:

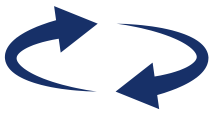
Carefully look at the email address:

- Is the domain correct?
- Is the name spelled correctly?
- (e.g., info@googleservices.com instead of info@google.com)



Look at the subject lines:

- Review subject lines carefully—look for misspellings, unnecessary capitalization, or suspicious characters that may indicate a phishing attempt



Some simple switches that hackers make:

- Switching out zero for the letter “O” or a capital “i” for a lowercase “L”.
- Adding a word that seems like it could be a subdomain of the real company.
- Ex: REAL - info@googleservice.cOm; FAKE - info@google.io

Common phishing attacks:

Unusual Activity: Suggests that someone gained access to your accounts and you need to change your password quickly. There are usually buttons that say, “Review recent activity” or “Click here to change your password.”

Fake Gift Cards: Someone sent you an e-gift card. The email redirects you to a website to ‘Claim gift card’ or ‘Redeem now.’

Account Verification Required: Suggests that your account has been disconnected, and that you need to verify your information. As soon as you enter your login credentials, the hacker has access.

Why is phishing so successful?

Because of social engineering - but what is it?

This refers to psychological manipulation used to bypass logic through emotional appeal—urgency, fear, trust, or curiosity. Attackers often impersonate CEOs, vendors, or banks to trick recipients.

Real life phishing scenario:

A 10-person company's owner worked remotely and let the office manager handle payroll and bills. Trusting her, he gave her access to his checking account. She received a convincing email, seemingly from the owner, instructing her to wire $50K. Without verifying, she followed the instructions and went to the bank.

Luckily, the bank intervened and called the owner. The incident occurred just as the company had begun cybersecurity training—despite passing a simulated phishing test, the office manager didn't take 30 seconds to verify the email.

Your #1 Vulnerability: Untrained Staff

Employees are often the weakest link in your cybersecurity chain—or your strongest defense. Without regular training, even the best firewalls or antivirus tools won't stop a successful phishing attack.

Why your firewall and anti-virus are not enough:

- Typical firewall does not filter outgoing traffic - when an employee clicks on a bad link, this is not filtered.
- Most phishing emails, malware and ransomware can easily bypass traditional antivirus software.
- You need next-generation endpoint detention, DNS filtering, and security awareness training on top of traditional antivirus and firewall.

Solution:

- DNS Filtering: Blocks access to malicious sites before a connection is established.
- Next-Generation Endpoint Protection: Goes beyond basic antivirus.
- Security Awareness Training: Helps employees recognize threats and respond appropriately.

Security Awareness Training

Typically comprised of sending consistent short training videos that explain a cybersecurity topic in a non-technical, easy-to-digest way. Ongoing security awareness training at least once per month. Security must always be top of mind; it must be ingrained in your company culture just like anything else. Training should be done in conjunction with simulated phishing campaigns.

- **Human errors cause almost 90% of data breaches** - employees are your first line of defense, the goal is to elevate their security posture.
- With security awareness training and stimulated phishing campaigns, you can reduce the risk of socially engineered cyberthreats by up to 80%.

What are simulated phishing campaigns?

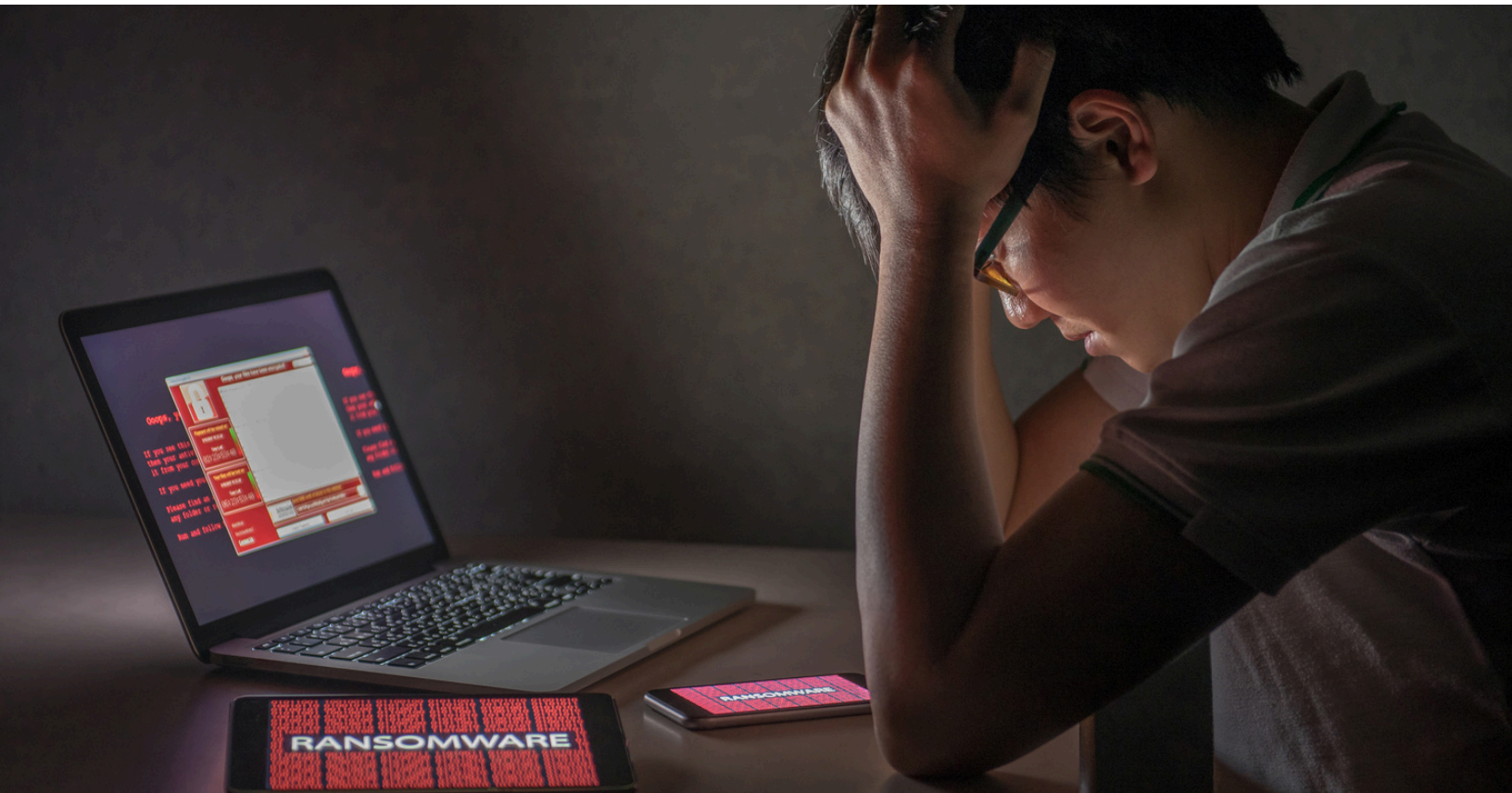
- Sent by IT staff
- Designed to trick an employee into clicking on a fake link
- If they do click (which means fail), they will be redirected to a security awareness training video to help them understand how they were duped.

How to Respond to a Cyberattack

What you do in the event of a cyberattack will depend on what you do before it.

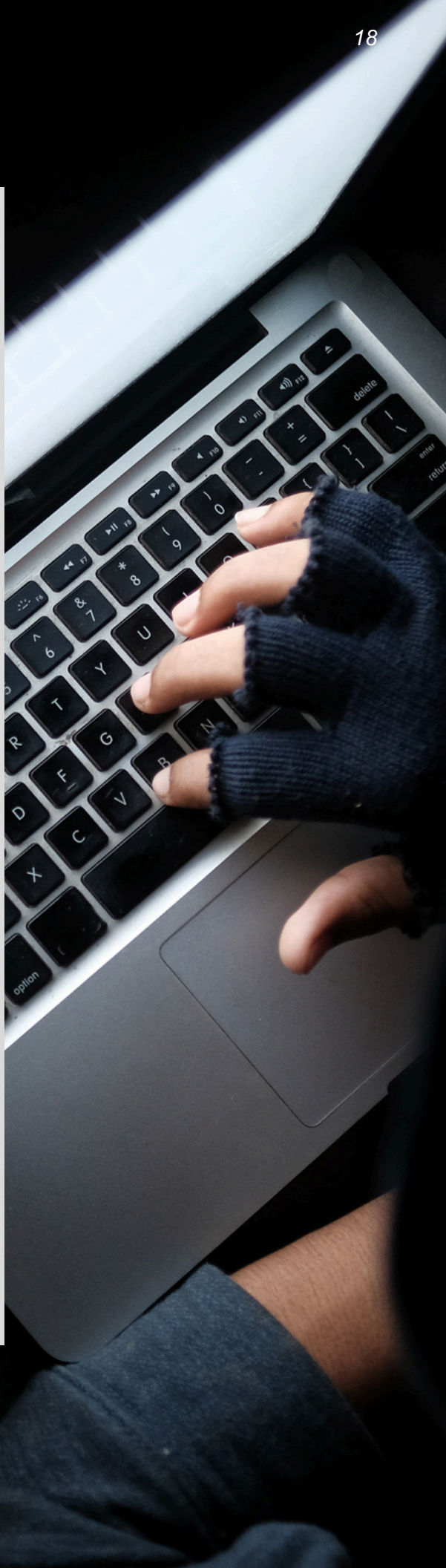
Preparation is key. If your organization experiences a breach, your response will only be as effective as your Business Continuity and Disaster Recovery (BCDR) Plan. The same preparations and procedures you would take in the event of a natural disaster, you will take in the event of a cyberattack. A BCDR plan ensures you are back up and running quickly.

The size and type of cyberattack will determine how many of the resources you will need to resolve this issue, but everything should be in place ahead of time. The Server Message Block (SMB) is a huge target. In your computer network, the SMB is responsible for sharing files, printers, and serial ports on a network. Hackers will manipulate the SMB via a worm tool or other form of malware in order to gain access to your devices.



6 warning signs you've been hit:

- Your browser redirects you to a different website than you intended.
- Your team members are receiving emails that you did not send, especially ones that relate to payments or transfer of funds.
- Your computer shows pop-ups with urgent notifications to let you know that your computer is infected, and you need to run a tool that you're not expecting or familiar with.
- Your computer slows down immediately after clicking something on the Internet, emails or other programs.
- Your inbox is suddenly overloaded with coupons or junk mail to a noticeable degree.
- Your clients report they made a payment to a new account, that you did not create or are not involved in.



You've Been Hacked: What Now?

Step 1: Remain calm.

Next, there are steps you can take to save your client's data, their trust, and your money.

Action Point 1: Document Everything
Before all else, you need to gather evidence so you can get help.

- Once you've determined you have been hacked, take screenshots or photos of any suspicious messages or errors.
- During the recovery process, keep a running diary and require that all members document steps taken.
- Part of the BCDR Plan should be the documentation and imaging of your network.

This should be a blueprint of your entire system, including software, software licenses, and the location of all hardware. This will assist when you need to re-establish your system post-attack.

Action Point 2: Identify the Source of the Breach
Now you can begin to identify the source of the breach and determine if the entire network is impacted, or if you can segregate the affected segment while maintaining the remainder of your operations.

Contact all necessary professionals:

- Your IT Consultant (us)
- Lawyer, in-house counsel
- Insurance provider

Action Point 3 - Disconnect from the internet

Unless we have said otherwise, disconnect from the internet until the virus/malware has been removed. Do not turn servers off -- they need to remain on so we can use the information to determine the source and solution. Once the virus/malware is completely removed, you can switch to backup servers.

RE: BACKUPS

Have caution relying on backups—there have been instances where hackers have adjusted the backup function so that you have unknowingly lost days, weeks, or months of data. To be safe follow the 3-2-1 Rule: 3 copies, 2 types of media, 1 copy offline.

Action Point 4: Critical Communication

Audience One: *Staff & Communications Tools*

Be judicious in communicating with staff on a “need-to-know" basis. Have someone develop a list of alternate communications options (private cell numbers and email addresses) so that you can communicate instructions.

Audience Two: *Clients*

Depending on your industry, you may have obligations to notify your clients. Follow the guidance of legal counsel with expertise in the laws governing your industry and jurisdiction. Some clients may have to be notified of new instructions on making payments. Make sure all clients know that any new payment instructions must be verified verbally with an employee known to them. (This policy should be in place before attack, and she be a regular practice)

Audience Three: *Stakeholders*

If you are a publicly traded company, you may have legal obligations to report significant incidents. It’s critical to be ready with a public statement regarding the event.

If ransom is involved:

I know we've all seen the crime shows, "You never pay the ransom!", and for the most part the same goes for cybersecurity attacks.

Consider this: If you make $1,000 per day in income and you need 6 days to repair the attack, you will lose $6,000. If the hackers ask for $3,000 in ransom, paying the ransom may make fiscal sense.

We only recommend making the ransom payment if you are prepared to immediately make changes that will protect against a second attack. If you do not have the proper tools in place, you will be compromised again, and likely for a higher ransom amount. Correcting any lapses in security is especially important once you have been attacked.

Cybersecurity Checklist: The Essential Layers

- ☐ Conduct regular security assessments
- ☐ Implement secure remote access protocols
- ☐ Minimize administrative privileges
- ☐ Develop an incident response plan
- ☐ Regularly backup your data
- ☐ Enforce security awareness training
- ☐ Review third-party vendor security
- ☐ Implement a thorough cyber security policy
- ☐ Regularly update software and hardware
- ☐ Regularly update antivirus and malware software
- ☐ Implement strong access controls
- ☐ Encrypt sensitive data
- ☐ Monitor and log network activity
- ☐ Establish a strong firewall configuration
- ☐ Develop a data classification system
- ☐ Implement intrusion detection & prevention systems
- ☐ Implement a mobile device policy
- ☐ Deploy email security measures
- ☐ Document all areas of the network

Conclusion

Cybersecurity is not a one-time project—it's an ongoing discipline. By creating a culture of security, educating your staff, and implementing layered protections, your business can defend itself against even the most sophisticated attacks.

Taking cybersecurity seriously protects more than data—it safeguards your reputation, your customers, and the future of your business.

About PC Professional

Since 1981, PC Professional has been dedicated to delivering comprehensive IT solutions to businesses and non-profit organizations throughout the Bay Area. Our offerings span a wide range of services, including managed and co-managed IT, cybersecurity, cloud solutions, and more.

Prioritizing prompt responses, we operate a 15-minute helpdesk response time to ensure swift client support. Our managed IT services encompass both remote and on-site assistance, focusing on security management, firewall protection, strategic planning, and network oversight. We also employ robust data protection strategies to secure digital assets and maintain a safe IT environment.

Discover more at www.pcprofessional.com or call (510) 874-5871.

PC Professional